IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	1:18CR492-1
	)	
	)	
TIMOTHY DONOVAN BURNS	)	

IN THE MATTER OF THE SEARCH OF	)	
A 2TB HITACHI HARD DRIVE,	)	1:18MJ307
SERIAL NUMBER YFGNBBTA	)	

MEMORANDUM OPINION AND ORDER

This matter comes before the undersigned United States Magistrate Judge on an Application for an Order to Require Defendant Burns to Assist in the Execution of a Search Warrant pursuant to the All Writs Act (the "Application") (1:18MJ307, Docket Entry 3).[1] For the reasons that follow, the undersigned Magistrate Judge will grant the Application.[2]

---

[1] Because (for reasons made apparent below) the execution of the search warrant at issue has not occurred, the docket (and each docket entry) in case number 1:18MJ307 remains sealed; however, the circumstances presented permit the disclosure in this Order of information about that search warrant and the Application.

[2] "[A] magistrate judge with authority in [a] district . . . has authority to issue a warrant to search for and seize . . . property located within th[at] district[.]" Fed. R. Crim. P. 41(b)(1). Additionally, in federal criminal cases, a magistrate judge may "determin[e] any matter that does not dispose of a charge or defense." Fed. R. Crim. P. 59(a); see also id. ("The magistrate judge must . . . enter on the record an oral or written order stating the determination."); Fed. R. Crim. P. 59(b)(1) (permitting

(continued...)

INTRODUCTION

On October 4, 2018, this Court (per the undersigned Magistrate Judge) issued a Search and Seizure Warrant (the "Warrant") for a 2TB Hitachi Hard Drive, Serial Number YFGNBBTA (the "Device"). (1:18MJ307, Docket Entry 2.) "The [D]evice . . . is related to the investigation of Timothy Donovan Burns . . . ." (Id., Attach. A.) The Warrant authorizes the search of the Device for (and seizure from the Device of) specified "evidence of . . ., the fruits of . . ., or property designed or intended for use or which has been used as the means of committing . . . violations of Title 18, United States Code, §[] 2252A(a)(5)(B)." (Id., Attach. B; see also id. (listing, as among items subject to seizure, "child pornography," "[r]ecords and information discussing or revealing sexual activity with or sexual interest in minors," "[r]ecords and

[2](...continued)
magistrate judges to issue only recommended rulings on "matter[s] that may dispose of a charge or defense"). Because the Application concerns execution of a search warrant (and not disposition of a charge or defense), the undersigned Magistrate Judge will issue an order (and not a recommendation). See United States v. Apple MacPro Computer, 851 F.3d 238, 245 (3d Cir. 2017) ("[T]he [m]agistrate [j]udge had subject matter jurisdiction under Federal Rule of Criminal Procedure 41 to issue a search warrant and therefore had jurisdiction to issue an order under the All Writs Act that sought to effectuate and prevent the frustration of that warrant." (internal footnote and quotation marks omitted)), cert. denied sub nom., Doe v. United States, U.S. , 138 S. Ct. 1988 (2018). "A party may serve and file objections to th[is O]rder within 14 days after being served with a copy . . . . The district judge must consider timely objections and modify or set aside any part of th[is O]rder that is contrary to law or clearly erroneous. Failure to object in accordance with this rule waives a party's right to review." Fed. R. Crim. P. 59(a).

information referencing or revealing the identity of individuals depicted in child pornography and the location depicted," and "[r]ecords and information referencing or revealing the trafficking of child pornography and those responsible").)

On December 17, 2018, a grand jury for this District indicted Burns for receiving and possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A) & (5)(B), respectively. (See 1:18CR492-1, Docket Entry 1 at 1-2.) The Indictment explicitly sought forfeiture of the Device, as "matter which contains . . . visual depiction[s described in Section 2252A and] . . . personal[property] used or intended to be used to commit or promote the commission of [the charged] offense[s], . . . in accordance with Title 18, United States Code, Section 2253, [Federal] Rule [of Criminal Procedure] 32.2, . . . and Title 28, United States Code, Section 2461(c)." (See id. at 2-3.)

On February 8, 2019, pursuant to a written Plea Agreement (signed by Burns and filed on January 30, 2019) (1:18CR492-1, Docket Entry 11) and a written Factual Basis (filed on February 5, 2019) (1:18CR492-1, Docket Entry 12), Burns pleaded guilty to receiving child pornography (before United States District Judge Loretta C. Biggs). (See 1:18CR492-1, Docket Entry dated Feb. 8, 2019.) In his Plea Agreement, Burns acknowledged that:

1) "[b]y pleading guilty . . ., [he] knowingly waive[d] and g[a]ve[] up his constitutional right[] . . . not to be compelled to incriminate himself" (1:18CR492-1, Docket Entry 11 at 4);

2) he "[wa]s going to plead guilty . . . because he [wa]s, in fact, guilty" (id. at 5);

3) he "knowingly consent[ed] and agree[d] to forfeit to the United States all right, title, and interest in and to any and all visual depictions described in . . . Section 2252A, and any and all property, real or personal, used or intended to be used to commit or to promote the commission of the offense [of receiving child pornography]" (id. at 6);

4) "[t]he property to be forfeited include[d] . . . [the Device]" (id.; see also id. at 7 ("knowingly and voluntarily waiv[ing] all constitutional . . . claims, defenses and challenges to the forfeiture of [the Device]")); and

5) "[n]o agreements, representations, or understandings ha[d] been made between the parties in this case other than those which [we]re explicitly set forth in th[at] Plea Agreement, and none w[ould] be entered into unless executed in writing and signed by all the parties" (id. at 10).

The Factual Basis for Burns's guilty plea establishes that:

1) law enforcement officers monitoring a computer-file-sharing network observed that someone using "IP address 174.111.32.203

. . . [i]n January and March 2018 . . . requested pieces of child pornography files" (1:18CR492-1, Docket Entry 12 at 6);[3]

2) "records obtained from [an internet service provider] revealed that IP address 174.111.32.203 resolved to 'Don Burns' at his apartment in Kernersville, North Carolina" (id.);[4]

3) "[o]n March 14, 2018, [North Carolina State Bureau of Investigation Criminal Specialist ('CS') Rodney] White and [a federal agent] traveled to Burns's apartment" (id. at 6-7);

4) "Burns answered the door and agreed to speak with the agents inside" (id. at 7);

---

[3] "When installing th[is n]etwork's software, each user agrees to provide to the [n]etwork a portion of the storage space on the user's computer hard drive, so that files uploaded by [the n]etwork['s] users can be distributed and stored across the [n]etwork." (1:18CR492-1, Docket Entry 12 at 1.) "When a user uploads a file into th[is n]etwork, the software breaks the file into pieces . . . and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the [n]etwork of [users]." (Id. at 2.) "When a user attempts to download a file via th[is n]etwork, the [n]etwork downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The [n]etwork software then requests all of the pieces of the file from the user's peers." (Id.) "[A] user who wishes to locate and download child pornography from th[is n]etwork must identify the key associated with a particular child pornography file and then use that key to download the file." (Id. at 3-4.) "[M]essage boards [on the network] contain [such] keys of child pornography files that can be downloaded through the [n]etwork." (Id. at 4.) "Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on th[is n]etwork. Law enforcement only investigates [the n]etwork['s] users who request pieces of files associated with such keys collected by law enforcement." (Id. at 5.)

[4] The name "Burns" appears in all-caps in the Factual Basis.

5) "[u]pon entry, the agents observed a desktop computer in the living room connected to a bay of hard drives" (id.);

6) "Burns explained that he lived alone and . . . formerly worked as a computer programmer" (id.);

7) "Burns admitted to using the [n]etwork [on which officers had observed his IP address requesting pieces of child pornography files]" (id.; see also id. ("Burns stated that he had been using [that network] for a few months."));

8) "[w]hen asked what he did with the child pornography files, Burns explained that he downloaded the files to a hard drive and then sorted through them, deleting the files he didn't want" (id. at 8; see also id. at 8-9 ("Burns said that he preferred minor girls 15 to 16 years of age. . . . CS White asked Burns which hard drive he used to save the child pornography that he downloaded. In response, Burns explained that there were three hard drives connected to his desktop computer. The first contained the computer's operating system, the second was the location to which files were downloaded, and the third contained music. During the interview with the agents, Burns sometimes qualified his answers by stating 'If I was doing it' and 'I'm not saying I did it' and then smiling." (internal ellipses omitted)));

9) "Burns denied using any type of encryption software to protect his files" (id. at 8);

10) "Burns gave CS White verbal consent to take [Burns's] computer and hard drives and examine them for child pornography" (id.; see also id. at 9 ("Burns [also] executed a written consent . . . . With Burns's permission, CS White took custody of the computer and hard drives."));

11) when "CS White forensically examined Burns's three computer hard drives," CS White discovered that "[t]he first . . . was in fact the computer's operating system and contained deleted child pornography files, the second, [the Device], was fully encrypted by VeraCrypt software, and the third did in fact contain music files" (id. at 9; see also id. ("The first hard drive, the operating system, contained 36 child pornography images that CS White recovered from unallocated space (i.e. they had been deleted from the active disk space).));

12) "the [first] hard drive's active space" contained "instructions on how to setup the [n]etwork . . . on a full disk encrypted hard drive" and on "how to use VeraCrypt software," as well as actual "VeraCrypt software" (id. at 9-10);

13) "[o]n March 20, 2018, the agents returned to Burns's residence to speak with him" and "Burns again agreed to speak with the agents inside" (id. at 10); and

14) CS White "asked for the password to the [Device]," after which "Burns unequivocally stated that there was child pornography on the [Device], but declined to provide the password because, as

he put it, letting the agents see the files would not be in his best interest" (id.).

At the time of Burns's guilty plea, he "agree[d] to participate in a Psychosexual Evaluation." (1:18CR492-1, Docket Entry dated Feb. 8, 2019.) According to records of the United States Probation Office, Psychosexual Evaluations:

1) "include a personal clinical interview, review [of] available court documents regarding the offense . . . [as well as] victim impact information, and utiliz[ation of] a battery of tests" (1:18CR492-1, Docket Entry 21 at 1; see also id. at 2 (stating that bar to "ask[ing] questions pertaining to the instant offense, or ask[ing] questions or administer[ing] tests that compel the defendant to make incriminating statements" applies only to "pretrial services defendants"), 3 (requiring evaluator to "review[] and consider[] . . . details of the current offense"));

2) "provide a written clinical evaluation of a defendant's[] risk for re-offending and current amenability for treatment; to guide and direct specific recommendations for the conditions of treatment and supervision of a defendant[]; to provide information that will help to identify the optimal setting, intensity of intervention, and level of supervision[; as well as] to assess the potential dangerousness of the defendant[]" (id. at 1); and

3) "shall consider . . . deviance and paraphilia, level and extent of pathology, deception and/or denial, . . . level of

violence and coercion, motivation and amenability for treatment, escalation of high-risk behaviors, risk of re-offense, treatment and supervision needs, and impact on the victim" (id.).[5]

Consistent with the foregoing guidance, the referral letter sent by the United States Probation Office to the entity performing Burns's Psychosexual Evaluation notes that agents acquired the Device from Burns (see 1:18CR492-1, Docket Entry 20 at 5), but found it "fully encrypted by Vera Crypt software" (id.), and that Burns later "unequivocally stated that there was child pornography on the hard drive, but declined to provide the password" (id. at 7; see also id. ("[Burns] stated letting the agents view the files would not be in his best interest. . . . The agents asked [Burns] why he was reluctant to provide the password given that [he] admitted to downloading and possessing child pornography. [He] again stated that it was not in his best interest to enable the agents to see the images stored on his hard drive.")).[6]

On February 25, 2019, the United States moved for entry of a forfeiture order as to the Device, on the ground that it "[wa]s

---

[5] The undersigned Magistrate Judge directed the Clerk to docket the above-cited document under seal, because it includes non-public information unnecessary to resolve the Application; however, the above-quoted material bears on such resolution and lacks characteristics that would preclude disclosure in this Order.

[6] The undersigned Magistrate Judge directed the Clerk to docket the above-cited document under seal, because it includes non-public information unnecessary to resolve the Application; however, the above-quoted material bears on such resolution and lacks characteristics that would preclude disclosure in this Order.

part and parcel of the offense to which [Burns] pled guilty, as described in the Factual Basis, and [Burns] has agreed to the forfeiture, [such that] the nexus requirement of Fed[eral] R[ule of] Crim[inal] P[rocedure] 32.2(b)(1) has been satisfied." (1:18CR492-1, Docket Entry 13 at 3.) By Order dated February 27, 2019, the Court (per Judge Biggs) expressly found the Device "forfeitable pursuant to . . . Section 2253(a)(1) and (a)(3), as property used in [and] intend[ed] to be used to commit or promote the commission of a violation of . . . Section 2252A(a)(2)(A) . . . ." (1:18CR492-1, Docket Entry 14 at 1; see also id. (declaring that, "based on the Plea Agreement and Factual Basis, there is a nexus between the [Device] and the offense [of receiving child pornography]," as well as that "publication is unnecessary because . . . the government has identified no persons who reasonably appear to be potential claimants").)

Shortly after Burns signed his Plea Agreement and just before Burns entered his guilty plea, the United States filed the Application, which "requests that the Court issue an order compelling [him] to produce [the Device] . . . in an unlocked and decrypted state." (1:18MJ307, Docket Entry 3 at 1.) After Burns pleaded guilty (and agreed to a Psychosexual Evaluation) and after the Court (per Judge Biggs) ordered the Device forfeited (pursuant to Burns's admissions in his Plea Agreement and matters documented in the Factual Basis), Burns responded in opposition to the

Application. (1:18CR492-1, Docket Entry 16 (the "Response").) The parties subsequently appeared for a hearing at which CS White testified (and confirmed the information in the Factual Basis), Burns presented no evidence, and counsel for each side argued. (See 1:18CR492-1, Docket Entry 17.)[7] As ordered at the end of the hearing, the United States thereafter filed a Supplemental Pleading regarding VeraCrypt. (1:18CR492-1, Docket Entry 18.)[8]

DISCUSSION

The United States has filed the "Application under the All Writs Act, . . . seek[ing] an order requiring Burns to assist in the effectuation of the [W]arrant . . . by producing the [Device] in a fully unlocked and unencrypted state." (1:18MJ307, Docket Entry 3 at 9.) In support of the request for such a decryption order, the Application states: "Upon issuance of the [W]arrant, [a federal agent] sent a forensic copy of the [Device] to [the United States Department of Homeland Security's] Cyber Crime Center. [The Cyber Crime Center] attempted to access the hard drive by means of

[7] The Clerk maintains an audio-recording of the hearing, which the undersigned Magistrate Judge recently reviewed to verify contemporaneously taken notes and to extract verbatim quotations.

[8] The undersigned Magistrate Judge permitted the filing of the Response and Supplemental Pleading under seal; however, nothing in them appears to merit such treatment. This Order thus will quote from those documents in resolving the Application and will require the parties to address the propriety of continued sealing.

brute-force decryption. To date, [those] efforts have been unsuccessful." (1:18MJ307, Docket Entry 3 at 8.)[9]

The All Writs Act authorizes this Court to "issue all writs necessary or appropriate in aid of [its] respective jurisdiction[] and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a); see also Pennsylvania Bureau of Corr. v. United States Marshals Serv., 474 U.S. 34, 43 (1985) ("The All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute."); Harris v. Nelson, 394 U.S. 286, 299 (1969) ("Th[e All Writs Act] has served since its inclusion, in substance, in the original Judiciary Act as a legislatively approved source of procedural instruments designed to achieve the rational ends of law." (internal quotation marks omitted)). "The power conferred by the [All Writs] Act extends, under appropriate circumstances, to persons who . . . are in a position to frustrate the implementation of a court order or the proper administration of justice . . . and encompasses even those who have not taken any affirmative action to hinder justice." United States v. New York Tel. Co., 434 U.S. 159, 174 (1977). In sum, the Court may "issue such commands under the All Writs Act as may be necessary or appropriate to effectuate and

[9] "'Brute-force attack' is [a] term of art in computer science used to describe a program designed to decode encrypted data by generating a large number of passwords." United States v. Phillips, 477 F.3d 215, 218 n.2 (5th Cir. 2007).

prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained[.]" Id. at 172.

"Here, the [undersigned] Magistrate Judge had subject matter jurisdiction under Federal Rule of Criminal Procedure 41 to issue [the W]arrant and therefore ha[s] jurisdiction to issue an order under the All Writs Act that s[eeks] 'to effectuate and prevent the frustration' of th[e W]arrant." United States v. Apple MacPro Computer, 851 F.3d 238, 245 (3d Cir. 2017) (quoting New York Tel., 434 U.S. at 172) (internal footnote omitted), cert. denied sub nom., Doe v. United States, U.S. , 138 S. Ct. 1988 (2018). More specifically, because "law enforcement could not decrypt the contents of th[e D]evice[], and [Burns] refused to comply [with a request to disclose the password to the Device], the [undersigned] Magistrate Judge [may] issue[] the [requested d]ecryption [o]rder pursuant to the All Writs Act." Id. at 246; see also id. (describing such a "[d]ecryption [o]rder" as "a necessary and appropriate means of effectuating the original search warrant").

Burns's Response challenges the foregoing analysis by arguing that the United States "has failed to show such a[decryption] order either necessary or appropriate. The description of the [Cyber Crime Center's] attempt to gain access to the [D]evice[] is vague at best and does not demonstrate a need so pressing as to be either necessary or appropriate . . . ." (1:18CR492-1, Docket Entry 16 at 2; see also id. at 5 ("The government has only shown

minimal attempts at decryption and has only mentioned rudimentary methods . . . . Furthermore, there is no evidence that the government has attempted to exploit weaknesses in the VeraCrypt Software in an effort to decrypt. The government has failed to prove the very basis of jurisdiction for relief under the All Writs Act: that such relief is necessary and appropriate.").) That argument falls short, because (at the hearing) CS White credibly testified about the significant decryption efforts made by law enforcement, including (unsuccessful) searches of the unencrypted hard drive containing Burns's computer operating system for password clues, research into possible weaknesses in VeraCrypt software (which revealed none), and details of the "brute-force attack" used by the Cyber Crime Center (which involved connecting the Device to powerful servers to continuously run "alpha-numeric combinations" of increasing length over the then-nearly six months since the Warrant's issuance). That evidence defeats any vagueness or insufficient-governmental-effort objection to the applicability of the All Writs Act and confirms the necessity and/or propriety of issuing a decryption order to Burns.

Next, Burns's Response opposes entry of the requested decryption order under the All Writs Act, on the ground that, "[b]y going to the third-party manufacturer[of VeraCrypt], the government could avoid [the] direct Fifth Amendment implications [of requiring him to produce the Device in an unencrypted form] and

possibly obtain the assistance the[government] need[s] . . . ." (Id. at 3; see also id. at 5 ("There is no evidence the government has contacted VeraCrypt (makers of the software at issue) or any other manufacturers for assistance with the decryption.").) The Supplemental Pleading filed by the United States forecloses that line of argument, in that it documents the public statements of VeraCrypt's France-based manufacturer, IDRIX, that:

> [IDRIX] ha[s] not implemented any "backdoor" in VeraCrypt (and will never implement any even if asked to do so by a government agency), because it would defeat the purpose of the software. VeraCrypt does not allow decryption of data without knowing the correct password or key. [IDRIX] cannot recover [a VeraCrypt user's] data because [IDRIX] do[es] not know and cannot determine the password [the user] chose or the key [the user] generated using VeraCrypt. The only way to recover [a VeraCrypt user's] files is to try to "crack" the password or the key, but it could take thousands or millions of years (depending on the length and quality of the password or keyfiles, on the software/hardware performance, algorithms, and other factors).

(1:18CR492-1, Docket Entry 18 at 2; see also id. at 3 ("[Counsel for Burns] does not object to the Court taking judicial notice of the assertions on the VeraCrypt or IDRIX websites.").) Given those undisputed facts, requiring the United States to seek decryption assistance from IDRIX (rather than Burns) would only further frustrate and delay effectuation of the Warrant.[10]

[10] To the extent Burns suggests that the Court should limit "[a]pplication of the All Writs Act to [] third part[ies] not at issue in the case" (1:18CR492-1, Docket Entry 16 at 5), the Court declines to adopt that view, given that "[t]he Supreme Court has explained . . . that [the All Writs] Act extends to anyone 'in a (continued...)

Nor (contrary to Burns's position (see 1:18CR492-1, Docket Entry 16 at 6-24)) does the Fifth Amendment's privilege against self-incrimination bar the Court from issuing the requested decryption order under the All Writs Act. "The relevant part of that Amendment provides: 'No person shall be [c]ompelled in any criminal case to be a [w]itness against himself.'" Fisher v. United States, 425 U.S. 391, 396 (1976) (quoting U.S. Const. amend. V) (internal ellipsis omitted). "Within the limits imposed by the language of the Fifth Amendment, . . . the privilege truly serves privacy interests; but the [Supreme] Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which . . . did not involve compelled testimonial self-incrimination of some sort." Id. at 399 (emphasis added); see also id. at 400-01 ("The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State's reason to believe incriminating evidence will be found becomes

[10](...continued)
position to frustrate the implementation of a court order or the proper administration of justice' as long as there are 'appropriate circumstances' for doing so," Apple MacPro, 851 F.3d at 246 (quoting New York Tel., 434 U.S. at 174) (emphasis added). Appropriate circumstances exist to direct the requested decryption order to Burns under the All Writs Act, because, "as in *New York Telephone*: (1) [Burns] is not 'far removed from the underlying controversy;' (2) 'compliance with [such a d]ecryption [o]rder requires minimal effort;' and (3) 'without [Burns's] assistance there is no conceivable way in which the [W]arrant . . . could be successfully accomplished.'" Id. (quoting New York Tel., 434 U.S. at 174-75) (internal brackets omitted).

sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment--the Fifth--to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination. We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy--a word not mentioned in its text and a concept directly addressed in the Fourth Amendment.").

Put another way, "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is [1] compelled to make [2] a [t]estimonial [c]ommunication [3] that is incriminating." Id. at 408 (emphasis added); see also Hiibel v. Sixth Judicial Dist. Ct. of Nev., Humboldt Cty., 542 U.S. 177, 189 (2004) ("To qualify for the Fifth Amendment privilege, a communication must be testimonial, incriminating, and compelled."). Accordingly, an individual "cannot avoid compliance with [a legal command to produce an item of evidence] merely by asserting that the item of evidence which he is required to produce contains incriminating [contents] . . . ." Fisher, 425 U.S. at 410; see also United States v. Hubbell, 530 U.S. 27, 35-36 (2000) ("[A] person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the

[Fifth Amendment] privilege."). "The act of producing evidence in response to a [legal command] nevertheless has communicative aspects of its own, wholly aside from the contents of the [evidence] produced." Fisher, 425 U.S. at 410; see also United States v. Doe, 465 U.S. 605, 612 (1984) ("Although the contents of a document may not be privileged, the act of producing the document may be."). In particular, an individual's "[c]ompliance with the [legal command to produce papers] tacitly concedes the existence of the papers demanded and their possession or control by the [individual]." Fisher, 425 U.S. at 410.

As to whether the act of producing an item of evidence in response to a legal command results in "compelled testimonial self-incrimination," id. at 399, the Supreme Court has stated that "[t]he element[] of compulsion [is] clearly present, but the more difficult issues are whether the tacit averments of the [compelled individual] are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment," id. at 410. The Supreme Court further has indicated that "resolution" of questions about those latter two elements often will "depend on the facts and circumstances of particular cases," id., but nonetheless has made clear that, when "[t]he existence and location of the papers are a forgone conclusion . . . [, the individual] adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers," id. at 411 (emphasis added).

Accordingly, "[u]nder th[o]se circumstances by enforcement of the [legal command] no constitutional rights are touched. The question is not of testimony but of surrender." Id. (internal quotation marks omitted); see also Apple MacPro, 851 F.3d at 247-48 (upholding application of "forgone conclusion" doctrine to Fifth Amendment challenge to decryption order entered under All Writs Act); In re Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1345-49 (11th Cir. 2012) (recognizing that "forgone conclusion" doctrine could defeat Fifth Amendment objection to grand jury subpoena's decryption demand, but concluding that record in that case did not satisfy all elements of doctrine).

In light of that authority and given the state of the record (documented in the Introduction and summarized below), Burns's "Fifth Amendment claim, based on the fact that . . . [the requested decryption order effectively] ask[s] for, and reveal[s his possession of], the password to the [Device], [thus] fails. Any self-incriminating testimon[ial communication] that [Burns] may have [to] provide[] by [enter]ing the password [i]s already a 'foregone conclusion' because the Government independently proved that [he] was the sole user and possessor of the [Device]." United States v. Gavegnano, 305 F. App'x 954, 956 (4th Cir. 2009). Moreover, to the extent that (contrary to the implications of the Fourth Circuit's ruling in Gavegnano), "where the government seeks decryption of hard drives," United States v. Spencer, No. 17CR259,

2018 WL 1964588, at *2 (N.D. Cal. Apr. 26, 2018) (unpublished), in order to defeat an assertion of Fifth Amendment privilege, "the government must show that it is a forgone conclusion not only that the defendant has the ability to decrypt the device(s), but also that certain files are on the device(s)," id. (recognizing that "Eleventh Circuit has [so] held" in In Re Grand Jury Subpoena, 670 F.3d at 1347); but see id. at *3 (rejecting Eleventh Circuit's view and holding that "the government need only show it is a forgone conclusion that [the defendant] has the ability to decrypt the devices")),[11] the record here (detailed in the Introduction) conclusively establishes that the Device contains child pornography files (including particularly contraband images of 15 and 16 year-old females) downloaded by Burns. By way of summary:

1) through the express terms of Burns's Plea Agreement (as subsequently endorsed at his plea hearing), Burns admitted not only

[11] Like the Spencer Court, the Third Circuit has declined to adopt the Eleventh Circuit's gloss on the "foregone conclusion" doctrine. See Apple MacPro, 851 F.3d at 248 n.7 ("[W]e are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order. Instead, a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the device is 'I, [the defendant], know the password for these devices.'"). In any event, even the Eleventh Circuit has held that, to satisfy the "forgone conclusion" doctrine in decryption cases, "the Government does not have to show that it knows specific file names." In re Grand Jury Subpoena, 670 F.3d at 1349 n.28.

that he received child pornography files, but also that he used the Device to receive child pornography files and/or that the Device contains child pornography files;[12]

2) the Factual Basis (and CS White's credible testimony) confirms that (A) during Burns's initial interview with law enforcement agents, he admitted that he lived alone, possessed computer expertise, and downloaded child pornography files to (and saved child pornography he liked, such as files with 15 and 16 year-old females, on) the Device, which he used in conjunction with a separate hard drive that housed his computer operating system, (B) a forensic review of the hard drive that Burns identified as containing his computer operating system verified that fact and revealed instructions for encrypting a hard drive and for using VeraCrypt software, as well as a copy of VeraCrypt software, (C) a forensic review of the Device could not proceed due to the encryption of all its contents with VeraCrypt software, and (D) during a follow-up interview with law enforcement agents, when asked for the password to decrypte the Device, Burns did not deny knowledge of the encryption or the decryption password and did not deny the presence of child pornography files on the Device, but

[12] At the hearing on March 19, 2019, Burns's counsel attempted to argue that, in negotiating the Plea Agreement, Burns intended to preserve the Fifth Amendment arguments raised in the Response; however, Burns's counsel acknowledged that the Plea Agreement lacks any such provision. Further, the Plea Agreement contains a clause denying the existence of any agreements outside the explicit terms of the Plea Agreement. (See 1:18CR492-1, Docket Entry 11 at 10.)

instead explicitly acknowledged the presence of child pornography files on the Device and declined to disclose the password because he believed that allowing law enforcement agents to view the files on the Device did not serve his interests;[13] and

3) based on Burns's admissions in his Plea Agreement and the uncontested information in the Factual Basis, the Court (per Judge Biggs) concluded that Burns used the Device to receive child pornography (and that he alone held any interest in the Device).

This record material belies the assertion in Burns's Response that "the contents of [the Device] are completely unknown to the[United States]" (1:18CR492-1, Docket Entry 16 at 16), as well as the Response's contention that "Burns never provided investigators with any evidence that he knew the password for the encrypted

---

[13] Notably, at the hearing on March 19, 2019, Burns's counsel conceded that, at the plea hearing, Burns did not contest the accuracy of the following sentences in the Factual Basis:

1) "When asked [during the first interview] what he did with the child pornography files, Burns explained that he downloaded the files to a hard drive and then sorted through them, deleting the files he didn't want." (1:18CR492-1, Docket Entry 12 at 8.);

2) "CS White asked Burns [during the first interview] which hard drive he used to save the child pornography that he downloaded. In response, Burns explained that there were three hard drives connected to his desktop computer. The first contained the computer's operating system, the second [i.e., the Device] was the location to which files were downloaded, and the third contained music." (Id. at 8-9.); and

3) "[During the second interview,] Burns unequivocally stated that there was child pornography on the [Device], but declined to provide the password because, as he put it, letting the agents see the files would not be in his best interest." (Id. at 10.)

device" (id. at 19 (emphasis added)) and that the Device "perhaps was encrypted by a previous user" (id.).[14] Such evidence also forecloses Burns's attempt to analogize this case to: (A) the Supreme Court's rejection of reliance on the "foregone conclusion" doctrine by the United States "in *Hubbell*, 530 U.S. at 44-45, [where the United States] had 'no prior knowledge of either the existence or whereabouts' (and th[u]s did not have sufficient evidence of possession) of the thousands of pages produced by the suspect in response to a [grand jury] subpoena" (1:18CR492-1, Docket Entry 16 at 17); and (B) the Eleventh Circuit's ruling in In Re Grand Jury Subpoena, 670 F.3d at 1346, "that the suspect's testimonial acts were not a foregone conclusion, in part because '[n]othing in the record illustrates that the government knows with reasonable particularity that the suspect is even capable of accessing the encrypted portions of the devices'" (1:18CR492-1, Docket Entry 16 at 20 (internal brackets omitted)).

As a last matter, the more hyperbolic flurries within Burns's Response – including that the United States has "ignore[d] the Fifth Amendment" (1:18CR492-1, Docket Entry 16 at 2), that construing the All Writs Act to authorize a decryption order "would fly right in the face of long standing Constitutional protections"

[14] Simply put, Burns's admissions that he used the Device to receive and store child pornography files he downloaded, as well as that the Device contained child pornography files, constitute compelling evidence that he knew the password for the Device and that he (not some previous user) encrypted the Device.

(id. at 4), that the Application "runs against the very foundation of our adversarial legal system" (id. at 24), and that "[f]orcing [] Burns to decrypt his devices is the functional equivalent of calling him to testify at trial by making him concede an element of the charged offense: possession" (id.) – warrant brief additional comment. First, the United States has not "ignored the Fifth Amendment" (id. at 2); to the contrary, after Burns signed a Plea Agreement admitting that he used the Device to receive and to save child pornography files, the United States filed a proper application with the Court in which it directly and reasonably addressed the "anticipate[d] . . . argu[ment] that an order requiring [Burns] to produce the [Device] in an unencrypted state violates his Fifth Amendment right against self-incrimination" (1:18MJ307, Docket Entry 3 at 13). (See id. at 13-22.)

Further, although non-frivolous arguments against issuance of decryption orders under the All Writs Act in general and/or of the decryption order specifically requested in this case may exist, as this Order shows, no "long standing Constitutional protections" (1:18CR492-1, Docket Entry 16 at 4) bar such use of the All Writs Act generally or render its specific application to Burns an affront to "the very foundation of our adversarial legal system" (id. at 24). Finally, whatever its implications, an order requiring Burns to decrypt the Device at this stage in the proceedings does not constitute "the functional equivalent of

calling him to testify at trial by making him concede an element of the charged offense: possession" (id.). As discussed above, Burns has pleaded guilty to receiving child pornography files and, in so doing, has admitted that he used the Device to download and to store those files. This Order thus merely recognizes that Burns already has conceded his possession of the Device and the child pornography files he placed thereon, while at the same time he has impeded the Warrant's lawful mandate for seizure of that contraband, by maintaining the Device's encryption.[15]

[15] Given Burns's "agree[ment] to participate in a Psychosexual Evaluation" (1:18CR492-1, Docket Entry dated Feb. 8, 2019), the continued inaccessibility of the Device impairs not only the ability of the United States "to access the [Device's] files so that [agents] could submit them to the National Center for Missing and Exploited Children (NCMEC) to determine if the children depicted had been identified" (1:18MJ307, Docket Entry 3 at 7) and so that agents could "confirm th[e accuracy of] Burns's statement that he had not produced any of the images" (id. at 8), but also the availability to the person performing the Psychosexual Evaluation of complete records "regarding the offense" (1:18CR492-1, Docket Entry 21 at 1), including "victim impact information" (id.) and "details of [Burns's] offense" (id. at 3), thereby undermining the evaluator's ability to properly complete a reliable "written clinical evaluation of [Burns's] risk of re-offending and current amenability for treatment" (id. at 1) and his "potential dangerousness" (id.), including as concerns his "level and extent of pathology, [as well as] deception and/or denial" (id.). Indeed, although the Docket reflects the recent filing of a report regarding Burns's Psychosexual Evaluation (1:18CR492-1, Docket Entry 19), that report cautions that "[t]he accuracy, opinions, and recommendations contained in th[e] report are limited by the accuracy of the self-reported information by [] Burns and the materials available to th[e] examiner at the time of th[e report's] writing" (id. at 1; see also id. at 1-2 ("Should any additional information come to light, th[e] examiner reserves the right to amend th[e] report or make modifications to any stated opinion or recommendation contained [t]herein.")).

CONCLUSION

The All Writs Act authorizes entry of an order requiring Burns to decrypt the Device to effectuate and/or to avoid frustration of the Warrant. The "forgone conclusion" doctrine defeats Burns's assertion of a Fifth Amendment privilege against entry of (and compliance with) such a decryption order.

IT IS THEREFORE ORDERED that the Application (1:18MJ307, Docket Entry 3) is **GRANTED**, in that, on or before May 28, 2019, Burns shall assist the United States in the execution of the Warrant (1:18MJ307, Docket Entry 2), as follows: the United States shall make the Device (or a forensic image thereof) available to Burns, who shall produce the Device (or forensic image thereof) in a fully unlocked and unencrypted state.

IT IS FURTHER ORDERED that, on or before May 28, 2019, the parties shall file a joint notice in case number 1:18CR492-1, setting out their shared or competing positions about the propriety of continued sealing of the Warrant (1:18MJ307, Docket Entry 2), the Application (1:18MJ307, Docket Entry 3), the Response (1:18CR492-1, Docket Entry 16), and the Supplemental Pleading (1:18CR492-1, Docket Entry 18), including (if either party contends that any such document should remain under seal) legal argument and authority justifying that position.

/s/ L. Patrick Auld
L. Patrick Auld
United States Magistrate Judge

May 10, 2019